(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113449285 A
(43)申请公布日 2021.09.28

(21)申请号 202110244319.9

(22)申请日 2021.03.05

(30)优先权数据
2020-052089 2020.03.24 JP

(71)申请人 株式会社东海理化电机制作所
地址 日本爱知县

(72)发明人 大桥洋介 古田昌辉 河野裕己
新田繁则

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王玮 闫月

(51)Int.Cl.
G06F 21/44(2013.01)
G06F 21/60(2013.01)

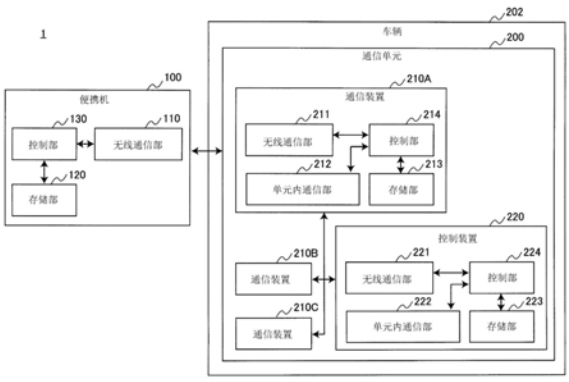
权利要求书3页 说明书18页 附图7页

(54)发明名称

认证系统以及认证方法

(57)摘要

本发明提供能够基于所测定的多个距离进行认证的构造。认证系统具备:多个通信装置;以及控制装置,基于由上述多个通信装置的每一个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理,上述多个通信装置的每一个具备无线通信部,上述无线通信部在与上述其他的通信装置之间进行无线通信,上述控制装置根据基于上述多个通信装置的每一个和上述其他的通信装置之间的无线通信而得到的上述多个通信装置的各个和上述其他的通信装置之间的距离所相关的信息的每一个,在多个上述距离所相关的信息的任一个满足规定条件的情况下,判定为上述其他的通信装置的认证成功。



CN 113449285 A

1.一种认证系统,所述认证系统具备:多个通信装置;以及控制装置,基于由所述多个通信装置的每一个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理,其特征在于,

所述多个通信装置的每一个具备无线通信部,所述无线通信部在与所述其他的通信装置之间进行无线通信,

所述控制装置根据基于所述多个通信装置的每一个和所述其他的通信装置之间的无线通信而得到的与所述多个通信装置的每一个和所述其他的通信装置之间的距离相关的信息亦即距离相关信息的每一个,在多个所述距离相关信息的任一个满足规定条件的情况下,判定为所述其他的通信装置的认证成功。

2.一种认证系统,所述认证系统具备:多个通信装置;以及控制装置,基于由所述多个通信装置的每一个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理,其特征在于,

所述多个通信装置的每一个具备无线通信部,所述无线通信部在与所述其他的通信装置之间进行无线通信,

所述控制装置根据基于所述多个通信装置的每一个和所述其他的通信装置之间的无线通信而得到的与所述多个通信装置的每一个和所述其他的通信装置之间的距离相关的信息亦即距离相关信息的每一个,在多个所述距离相关信息的全部不满足规定条件的情况下,判定为所述其他的通信装置的认证不成立。

3.根据权利要求1所述的认证系统,其特征在于,

所述控制装置在多个所述距离相关信息的全部不满足规定条件的情况下,判定为所述其他的通信装置的认证不成立。

4.根据权利要求1～3中任一项所述的认证系统,其特征在于,

所述距离相关信息是所述距离。

5.根据权利要求4所述的认证系统,其特征在于,

所述多个通信装置的每一个计算所述距离,

所述控制装置判定所述距离是否满足所述规定条件,判定所述其他的通信装置的认证成功与否。

6.根据权利要求1～3中任一项所述的认证系统,其特征在于,

所述距离相关信息是用于计算所述距离的时间长度。

7.根据权利要求6所述的认证系统,其特征在于,

所述多个通信装置的每一个获取所述时间长度,

所述控制装置基于所述时间长度计算所述距离,判定所计算出的所述距离是否满足所述规定条件,判定所述其他的通信装置的认证成功与否。

8.根据权利要求1～3中任一项所述的认证系统,其特征在于,

所述距离相关信息是用于计算所述距离的时刻。

9.根据权利要求8所述的认证系统,其特征在于,

所述多个通信装置的每一个获取所述时刻,

所述控制装置基于所述时刻而获取用于计算所述距离的时间长度,基于所述时间长度而计算所述距离,判定所述距离是否满足所述规定条件,判定所述其他的通信装置的认证

成功与否。

10.根据权利要求1～3中任一项所述的认证系统,其特征在于,

所述距离相关信息是表示所述距离是否满足所述规定条件的信息。

11.根据权利要求10所述的认证系统,其特征在于,

所述多个通信装置的每一个计算所述距离,判定所述距离是否满足所述规定条件,

所述控制装置基于表示所述距离是否满足所述规定条件的信息,来判定所述其他的通信装置的认证成功与否。

12.根据权利要求1～11中任一项所述的认证系统,其特征在于,

所述多个通信装置包含第一通信装置以及一个以上的第二通信装置,

所述一个以上的第二通信装置的每一个与所述第一通信装置连接,并发送所述距离相关信息,

所述第一通信装置与所述一个以上的第二通信装置的每一个以及所述控制装置连接,发送由所述第一通信装置得到的所述距离相关信息、以及从所述一个以上的第二通信装置的每一个接收到的所述距离相关信息中的至少任一个所对应的信息亦即对应信息。

13.根据权利要求12所述的认证系统,其特征在于,

所述距离相关信息是表示所述距离是否满足所述规定条件的信息,

所述第一通信装置将表示在所述多个通信装置的任一个中所述距离是否满足规定条件的信息作为所述对应信息发送。

14.根据权利要求13所述的认证系统,其特征在于,

所述第一通信装置在从所述第二通信装置接收所述距离相关信息之前计算所述距离,在所计算出的所述距离满足所述规定条件的情况下,将表示所述距离满足所述规定条件的信息作为所述对应信息发送。

15.根据权利要求13或14所述的认证系统,其特征在于,

所述第二通信装置预先生成表示所述距离是否满足所述规定条件的信息的候选,将所计算出的所述距离所对应的所述候选作为所述距离相关信息发送。

16.根据权利要求13～15中任一项所述的认证系统,其特征在于,

所述第一通信装置预先生成所述对应信息的候选,将所计算出的所述距离以及从所述第二通信装置接收到的所述距离相关信息所对应的所述候选作为所述对应信息发送。

17.根据权利要求16所述的认证系统,其特征在于,

所述第一通信装置预先生成所述距离相关信息的候选,发送所生成的所述候选与从所述第二通信装置接收到的所述距离相关信息的比较结果所对应的所述对应信息。

18.根据权利要求16或17所述的认证系统,其特征在于,

所述控制装置预先生成所述对应信息的候选,根据所生成的所述候选与从所述第一通信装置接收到的所述对应信息的比较结果,进行所述其他的通信装置的认证。

19.根据权利要求12～18中任一项所述的认证系统,其特征在于,

在接收到的所述距离相关信息不正当的情况下,所述第一通信装置将表示接收到的所述距离相关信息不正当的信息作为所述对应信息发送。

20.根据权利要求12～19中任一项所述的认证系统,其特征在于,

所述第一通信装置对所述对应信息进行加密而发送,

所述一个以上的所述第二通信装置的每一个对所述距离相关信息进行加密而发送。

21.根据权利要求1～11中任一项所述的认证系统,其特征在于,

所述多个通信装置的每一个与所述控制装置连接,在执行了对直至所述控制装置的通信路径的空闲进行确认的载波侦听的基础上发送所述距离相关信息。

22.根据权利要求1～11中任一项所述的认证系统,其特征在于,

所述多个通信装置的每一个与所述控制装置连接,在预先分配给所述多个通信装置的每一个的时机发送所述距离相关信息。

23.根据权利要求21或22所述的认证系统,其特征在于,

所述多个通信装置的每一个预先生成表示所述距离是否满足所述规定条件的信息的候选,将计算出的所述距离所对应的所述候选作为所述距离相关信息发送。

24.根据权利要求23所述的认证系统,其特征在于,

所述控制装置预先生成所述距离相关信息的候选,根据所生成的所述候选与从所述多个通信装置的每一个接收到的所述距离相关信息的比较结果,进行所述其他的通信装置的认证。

25.根据权利要求21～24中任一项所述的认证系统,其特征在于,

所述多个通信装置的每一个对所述距离相关信息进行加密而发送。

26.根据权利要求1～25中任一项所述的认证系统,其特征在于,

所述多个通信装置搭载于车辆,

所述其他的通信装置是由所述车辆的用户携带的装置。

27.一种认证方法,所述认证方法由系统执行,所述系统具备:多个通信装置;以及控制装置,基于由所述多个通信装置的每一个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理,其特征在于,

所述认证方法包括:

所述多个通信装置的每一个在与所述其他的通信装置之间进行无线通信;

所述控制装置根据基于所述多个通信装置的每一个和所述其他的通信装置之间的无线通信而得到的与所述多个通信装置的每一个和所述其他的通信装置之间的距离相关的信息亦即距离相关信息的每一个,在多个所述距离相关信息的任一个满足规定条件的情况下,判定为所述其他的通信装置的认证成功。

28.一种认证方法,所述认证方法由系统执行,所述系统具备:多个通信装置;以及控制装置,基于由所述多个通信装置的每一个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理,其特征在于,

所述多个通信装置的每一个在与所述其他的通信装置之间进行无线通信;

所述控制装置根据基于所述多个通信装置的每一个和所述其他的通信装置之间的无线通信而得到的与所述多个通信装置的每一个和所述其他的通信装置之间的距离相关的信息亦即距离相关信息的每一个,在多个所述距离相关信息的全部不满足规定条件的情况下,判定为所述其他的通信装置的认证不成立。

认证系统以及认证方法

技术领域

[0001] 本发明涉及认证系统以及认证方法。

背景技术

[0002] 近年来，测定装置间的距离的测距技术被利用于各种服务。例如，在下述专利文献1中，公开了如下技术：测定车辆与便携机之间的距离，根据所测定的距离来判定车门的上锁或解锁的可否，或者警告车门打开。

[0003] 专利文献1：日本特开2014-51809号公报

[0004] 在上述专利文献1所记载的技术中，测定一个车辆与便携机之间的距离，用于车门的上锁或者解锁等服务。但是，关于测定多个距离并用于服务的情况，没有进行任何研究。

发明内容

[0005] 因此，本发明是鉴于上述问题而完成的，本发明的目的在于提供一种能够基于所测定的多个距离进行认证的构造。

[0006] 为了解决上述课题，根据本发明的一个观点，提供一种认证系统，上述认证系统具备：多个通信装置；以及控制装置，基于由上述多个通信装置的各个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理，上述多个通信装置的各个具备在与上述其他的通信装置之间进行无线通信的无线通信部，上述控制装置根据基于上述多个通信装置的各个和上述其他的通信装置之间的无线通信而得到的与上述多个通信装置的各个和上述其他的通信装置之间的距离相关的信息的每一个，在多个与上述距离相关的信息的任一个满足规定条件的情况下，判定为上述其他的通信装置的认证成功。

[0007] 另外，为了解决上述课题，根据本发明的另一观点，提供一种认证系统，上述系统具备：多个通信装置；以及控制装置，基于由上述多个通信装置的各个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理，上述多个通信装置的各个具备在与上述其他的通信装置之间进行无线通信的无线通信部，上述控制装置根据基于上述多个通信装置的各个和上述其他的通信装置之间的无线通信而得到的与上述多个通信装置的各个和上述其他的通信装置之间的距离相关的信息的每一个，在多个与上述距离相关的信息的全部不满足规定条件的情况下，判定为上述其他的通信装置的认证不成立。

[0008] 另外，为了解决上述课题，根据本发明的另一观点，提供一种认证方法，该认证方法由系统执行，上述系统具备：多个通信装置；以及控制装置，基于由上述多个通信装置的各个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理，上述认证方法包括：上述多个通信装置的各个在与上述其他的通信装置之间进行无线通信；上述控制装置根据基于上述多个通信装置的各个和上述其他的通信装置之间的无线通信而得到的与上述多个通信装置的各个和上述其他的通信装置之间的距离相关的信息的每一个，在多个与上述距离相关的信息的任一个满足规定条件的情况下，判定为上述其他的通信装置的认证成功。

[0009] 另外，为了解决上述课题，根据本发明的另一观点，提供一种认证方法，该认证方法由系统执行，上述系统具备：多个通信装置；以及控制装置，基于由上述多个通信装置的各个与不同于该多个通信装置的其他的装置之间的无线通信而得到的信息来执行处理，上述认证方法包括：上述多个通信装置的各个在与上述其他的通信装置之间进行无线通信；上述控制装置根据基于上述多个通信装置的各个和上述其他的通信装置之间的无线通信而得到的与上述多个通信装置的各个和上述其他的通信装置之间的距离相关的信息的每一个，在多个与上述距离相关的信息的全部不满足规定条件的情况下，判定为上述其他的通信装置的认证不成立。

[0010] 如以上说明，根据本发明，提供能够基于所测定的多个距离进行认证的构造。

附图说明

[0011] 图1是表示本发明的一个实施方式所涉及的系统的结构的一个例子的图。

[0012] 图2是表示本实施方式所涉及的系统中所执行的请求响应认证的流程的一个例子的时序图。

[0013] 图3是表示本实施方式所涉及的系统中所执行的测距处理的流程的一个例子的时序图。

[0014] 图4是表示本实施方式所涉及的通信单元中所执行的第二认证处理的基本的流程的一个例子的流程图。

[0015] 图5是表示本实施方式所涉及的通信装置与控制装置的第一连接方式的框图。

[0016] 图6是表示本实施方式所涉及的通信装置与控制装置的第二连接方式的框图。

[0017] 图7是表示本实施方式所涉及的通信装置与控制装置的第三连接方式的框图。

[0018] 图8是表示本实施方式所涉及的主机与从机之间的信息的流程的一个例子的图。

[0019] 图9是表示本实施方式所涉及的控制装置与主机之间的信息的流程的一个例子的图。

[0020] 图10是表示本实施方式所涉及的通信单元中的信息的流程的一个例子的图。

[0021] 图11是表示本实施方式所涉及的通信单元中所执行的第二认证处理的详细的流程的一个例子的时序图。

[0022] 附图标记说明

[0023] 1…系统；100…便携机；110…无线通信部；120…存储部；130…控制部；200…通信单元；202…车辆；210…通信装置；211…无线通信部；212…单元内通信部；213…存储部；214…控制部；220…控制装置；221…无线通信部；222…单元内通信部；223…存储部；224…控制部。

具体实施方式

[0024] 以下参照附图并对本发明的优选的实施方式进行详细说明。此外，在本说明书以及附图中，对于实质上具有相同的功能结构的构成要素，标注相同的附图标记从而省略重复说明。

[0025] 另外，在本说明书以及附图中，有时也在相同的附图标记后标注不同的字母来区别实质上具有相同的功能结构的要素。例如，根据需要如通信装置210A、210B以及210C那样

区别实质上具有相同的功能结构的多个要素。但是，在不需要特意区别实质上具有相同的功能结构的多个要素的各个的情况下，仅标注相同的附图标记。例如，在不需要特意区别通信装置210A、210B以及210C的情况下，简称为通信装置210。

[0026] ＜＜1.结构例＞＞

[0027] 图1是表示本发明的一个实施方式所涉及的系统1的结构的一个例子的图。如图1所示，本实施方式所涉及的系统1包括便携机100、以及通信单元200。本实施方式中的通信单元200搭载于车辆202。车辆202是用户的利用对象的一个例子。

[0028] 在本发明中涉及被认证者侧的装置和认证者侧的装置。便携机100是被认证者侧的装置的一个例子。通信单元200是认证者侧的装置的一个例子。系统1也被称为认证系统。

[0029] 若用户(例如，车辆202的驾驶员)携带便携机100接近车辆202，则在便携机100与通信单元200之间进行用于认证的无线通信。而且，若认证成功，则车辆202的车门锁被解锁或发动机被启动，车辆202变成能够由用户利用的状态。系统1也被称为智能钥匙系统。以下，对各构成要素依次进行说明。

[0030] (1)便携机100

[0031] 便携机100是第一通信装置的一个例子。便携机100构成为由用户携带的任意的装置。作为任意的装置，列举有电子钥匙、智能手机、以及可穿戴终端等。

[0032] 如图1所示，便携机100具备无线通信部110、存储部120、以及控制部130。

[0033] 无线通信部110具有在与通信单元200之间进行以依据规定的无线通信标准的通信的功能。无线通信部110例如构成为能够进行依据第一无线通信标准以及第二无线通信标准的通信的通信接口。

[0034] 第一无线通信标准与第二无线通信标准相比，也可以满足增益高以及接收侧的功率消耗低中的至少任一个。

[0035] 作为满足这些必要条件的具体例，在第二无线通信标准中，也可以使用频率比第一无线通信标准中的载波的频率高的载波。这是因为载波的频率越高对应于距离的衰减越大，因此增益变低，载波的频率越低对应于距离的衰减越小，因此增益变高，满足关于增益的上述必要条件。

[0036] 另外，若载波的频率高，则基于人体的吸收等人体影响变大，增益降低。

[0037] 此外，如果考虑根据载波的频率的最大值来设定采样频率，则至少满足第二无线通信标准中的载波的最大频率比第一无线通信标准中的载波的最大频率高的情况即可。

[0038] 例如，在第一无线通信标准中，也可以使用超短波(UHF:Ultra-High Frequency:超高频)以及长波(LF:Low Frequency:低频)带的信号。在典型的智能钥匙系统中，在从便携机100向通信单元200的发送中使用UHF带的信号，在从通信单元200向便携机100的发送中使用LF带的信号。无线通信部110在向通信单元200的发送中能够使用UHF带的信号。另外，无线通信部110能够从通信单元200接收LF带的信号。

[0039] 例如，在第二无线通信标准中，也可以使用利用了UWB(Ultra-Wide Band:超宽带)的信号。基于UWB的脉冲方式的信号具有能够高精度地进行测距这样的特性。即，基于UWB的脉冲方式的信号通过使用纳秒以下的非常短的脉冲宽度的电波，能够高精度地测定电波的空中传播时间，并能够高精度地进行基于传播时间的测距。在这里，测距是指测定收发信号的装置间的距离。由测距测定的距离也被称为测距值。另外，进行测距的处理也被称为测距

处理。

[0040] 存储部120具有存储用于便携机100的动作的各种信息的功能。例如，存储部120存储用于便携机100的动作的程序、以及用于认证的ID(identifier:识别符)、密码、以及认证算法等。存储部120例如由闪存等存储介质、以及执行向存储介质的记录再现的处理装置构成。

[0041] 控制部130具有控制基于便携机100的全部动作的功能。作为一个例子，控制部130控制无线通信部110进行与通信单元200的通信。另外，控制部130进行从存储部120读取信息以及向存储部120写入信息。控制部130例如由CPU(Central Processing Unit:中央处理器)以及微处理器等电子电路构成。

[0042] (2)通信单元200

[0043] 通信单元200与车辆202对应设置。在这里，通信单元200搭载于车辆202。作为搭载位置的例子，列举有在车辆202的车室内设置通信单元200、或者通信单元200作为通信模块内置于车辆202等。如图1所示，通信单元200具备多个通信装置210(210A～210C)以及控制装置220。

[0044] 通信装置210

[0045] 通信装置210是在与便携机100之间进行无线通信的装置。

[0046] 如图1所示，通信装置210A具备无线通信部211、单元内通信部212、存储部213、以及控制部214。此外，通信装置210B以及通信装置210C具备与通信装置210A同样的构成要素。

[0047] 无线通信部211具有在与便携机100之间进行依据规定的无线通信标准的通信的功能。无线通信部211例如构成为能够进行依据第二无线通信标准的通信的通信接口。即，无线通信部211收发使用了UWB的信号。

[0048] 单元内通信部212具有在与通信单元200所包含的其他的装置之间进行通信的功能。作为一个例子，单元内通信部212在与控制装置220之间进行通信。作为另外的一个例子，单元内通信部212在与其他的通信装置210之间进行通信。单元内通信部212例如构成为LIN(Local Interconnect Network:局域互联网络)或CAN(Controller Area Network:控制器域网)等的能够进行依据任意的车载网络的标准的通信的通信接口。

[0049] 存储部213具有存储用于通信装置210的动作的各种信息的功能。例如，存储部213存储用于通信装置210的动作的程序、以及用于认证的ID(identifier:标识符)、密码、以及认证算法等。存储部213例如由闪存等存储介质、以及执行向存储介质的记录再现的处理装置构成。

[0050] 控制部214具有控制基于通信装置210的动作的功能。作为一个例子，控制部214控制无线通信部211在与便携机100之间进行通信。作为另外的一个例子，控制部214控制单元内通信部212而在与通信单元200所包含的其他的装置之间进行通信。作为另外的一个例子，控制部214进行从存储部213读取信息以及向存储部213写入信息。控制部214例如构成为ECU(Electronic Control Unit:电子控制单元)。

[0051] 控制装置220

[0052] 控制装置220是基于由多个210的各个和不同于该多个通信装置210的其他的通信装置亦即便携机100之间的无线通信而得到的信息来执行处理的装置。

[0053] 如图1所示，控制装置220具备无线通信部221、单元内通信部222、存储部223、以及控制部224。

[0054] 无线通信部221具有在与便携机100之间进行无线通信的功能。无线通信部221例如构成为能够进行依据第一无线通信标准的通信的通信接口。即，无线通信部221发送LF带的信号。另外，无线通信部221接收UHF带的信号。

[0055] 单元内通信部222具有在与通信单元200所包含的其他的装置之间进行通信的功能。作为一个例子，单元内通信部222在与通信装置210之间进行通信。单元内通信部222例如构成为LIN(Local Interconnect Network:局域互联网络)或CAN(Controller Area Network:控制器域网)等的能够进行依据任意的车载网络的标准的通信的通信接口。

[0056] 存储部223具有存储用于控制装置220的动作的各种信息的功能。例如，存储部223存储用于控制装置220的动作的程序、以及用于认证的ID(identifier)、密码、以及认证算法等。存储部223例如由闪存等存储介质、以及执行向存储介质的记录再现的处理装置构成。

[0057] 控制部224具有控制基于控制装置220的动作的功能。作为一个例子，控制部224控制无线通信部221而在与便携机100之间进行通信。作为另外的一个例子，控制部224控制单元内通信部222而在与通信单元200所包含的其他的装置之间进行通信。作为另外的一个例子，控制部224进行从存储部223读取信息以及向存储部223写入信息。控制部224例如构成为ECU(Electronic Control Unit:电子控制单元)。

[0058] 尤其，控制部224执行基于由多个210的各个与便携机100之间的无线通信而得到的信息的处理。该处理也可以进一步基于由控制装置220与便携机100之间的无线通信而得到的信息来执行。

[0059] 该处理的一个例子是认证便携机100的认证处理。该处理的另外的一个例子是车辆202的车门锁的上锁以及解锁等的控制车门锁的处理。该处理的另外的一个例子是车辆202的发动机的启动/停止等的控制动力源的处理。此外，车辆202所具备的动力源除了发动机以外也可以是马达等。

[0060] ＜＜2.技术的特征＞＞

[0061] ＜2.1.基本的特征＞

[0062] (1)两阶段认证

[0063] 本实施方式所涉及的便携机100以及车辆202的通信单元200阶段性地进行多个认证处理。作为一个例子，在这里进行两阶段认证。

[0064] 第一阶段的认证处理(以下，也称为第一认证处理)例如包括请求响应认证。所谓请求响应认证是认证者生成认证请求并发送到被认证者，被认证者基于认证请求生成认证响应并发送到认证者，认证者基于认证响应进行被认证者的认证的认证方式。认证请求是请求认证所需的信息的回答的信号。认证响应是基于认证请求以及被认证者的信息(例如，ID以及密码等)生成的数据。典型地，认证请求是随机数，在每次认证时变化，因此请求响应认证对反射攻击具有抗性。另外，认证响应基于被认证者的信息(例如，ID以及密码等)被生成，即ID以及密码本身不被收发，因此防止窃听。

[0065] 在第一认证处理之后进行的第二阶段的认证处理(以下，也称为第二认证处理)例如是基于距离的认证。基于距离的认证包括测定便携机100与通信单元200之间的距离的处

理即测距处理、以及基于作为距离的测定结果的测距值进行认证的处理。在第二认证处理中，根据测距值是否满足规定条件来进行认证。例如，测距值如果在规定值以下则认证成功，否则认证失败。

[0066] 这样，通过阶段性地进行多个认证处理，能够更强化安全性。

[0067] 也可以在第一认证处理之前，进行收发指示启动的唤醒信号、以及针对唤醒信号的响应。通过唤醒信号，能够使接收侧从睡眠状态复原。作为针对唤醒信号的响应，列举有表示启动的肯定响应(ACK:Acknowledgement)信号、以及表示不启动的否定响应(NACK:Negative Acknowledgement)信号。

[0068] (2)请求响应认证

[0069] 在请求响应认证中，作为一个例子，进行依据第一无线通信标准的通信。这是因为，在请求响应认证中，由于收发数据的关系，优选使用增益高的无线通信标准。

[0070] 以下，参照图2并对请求响应认证的流程的一个例子进行说明。

[0071] 图2是表示本实施方式所涉及的系统1中所执行的请求响应认证的流程的一个例子的时序图。如图2所示，在本时序图中，涉及便携机100以及控制装置220。

[0072] 如图2所示，首先，控制装置220的无线通信部221发送指示便携机100的启动的唤醒信号(步骤S102)。唤醒信号也可以作为UHF/LF带的信号被发送。

[0073] 便携机100的无线通信部110若接收唤醒信号，则发送作为唤醒信号的响应的ACK信号(步骤S104)。ACK信号也可以作为UHF/LF带的信号被发送。

[0074] 接着，控制装置220的控制部224生成认证请求。接下来，控制装置220的无线通信部221发送所生成的包含认证请求的信号(步骤S106)。包含认证请求的信号也可以作为UHF/LF带的信号被发送。

[0075] 对于便携机100的控制部130而言，若无线通信部110接收包含认证请求的信号，则基于所接收的认证请求生成认证响应。而且，便携机100的无线通信部110发送所生成的包含认证响应的信号(步骤S108)。包含认证响应的信号也可以作为UHF/LF带的信号被发送。

[0076] 对于控制装置220的控制部224而言，若无线通信部221接收包含认证响应的信号，则基于所接收的认证响应进行便携机100的认证(步骤S110)。

[0077] (3)测距处理

[0078] 在测距处理中，作为一个例子，进行依据第二无线通信标准的通信。这是因为，尤其通过使用基于UWB的脉冲方式的信号，能够高精度地进行基于传播时间的测距。测距处理包括收发用于测距处理的信号、以及基于收发用于测距处理的信号而得到的信息来计算测距值。

[0079] 为了测距处理而进行收发的信号的一个例子是测距用信号。测距用信号是为了测定装置间的距离而进行收发的信号。测距用信号也是成为计测的对象的信号。例如，测距用信号的收发所需的时间被计测。测距用信号典型地由不具有储存数据的有效负载部分的帧格式构成。除此之外，测距用信号也可以由具有有效负载部分的帧格式构成。

[0080] 在测距处理中，能够在装置间收发多个测距用信号。将多个测距用信号中的从一方的装置向另一方的装置发送的测距用信号也称为第一测距用信号。而且，将从接收第一测距用信号的装置向发送第一测距用信号的装置发送的测距用信号也称为第二测距用信号。

[0081] 为了测距处理而进行收发的信号的另外的一个例子是数据信号。数据信号是储存数据而进行输送的信号。数据信号由具有储存数据的有效负载部分的帧格式构成。

[0082] 在测距处理中，在以下将收发测距用信号、以及数据信号也称为测距通信。

[0083] 以下，参照图3并对测距处理的流程的一个例子进行说明。

[0084] 图3是表示本实施方式所涉及的系统1中所执行的测距处理的流程的一个例子的时序图。如图3所示，在本时序图中涉及便携机100以及通信装置210。

[0085] 如图3所示，首先，便携机100的无线通信部110发送第一测距用信号(步骤S202)。第一测距用信号作为使用了UWB的信号被发送。

[0086] 通信装置210的无线通信部211若从便携机100接收第一测距用信号，则发送作为第一测距用信号的响应的第二测距用信号(步骤S204)。第二测距用信号作为使用了UWB的信号被发送。

[0087] 对于便携机100的控制部130而言，若无线通信部110接收第二测距用信号，则计测从第一测距用信号的发送时刻到第二测距用信号的接收时刻的时间ΔT1。接着，便携机100的无线通信部110发送包含对表示所计测的ΔT1的信息进行加密后的信息的数据信号(步骤S206)。数据信号作为使用了UWB的信号被发送。

[0088] 另一方面，通信装置210的控制部214预先计测从第一测距用信号的接收时刻到第二测距用信号的发送时刻的时间ΔT2。而且，对于通信装置210的控制部214而言，若无线通信部211从便携机100接收数据信号，则基于由所接收的数据信号表示的ΔT1和所计测的ΔT2，获取表示便携机100与通信装置210之间的距离的测距值(步骤S208)。例如，首先，通过将ΔT1－ΔT2除以2来计算传播时间。这里的传播时间是便携机100与通信装置210之间的单程的信号收发所需的时间。而且，通过将传播时间乘以信号的速度，从而计算表示便携机100与通信装置210之间的距离的测距值。

[0089] (4)基于测距值的认证

[0090] 控制装置220根据基于多个通信装置210的各个与便携机100之间的无线通信而得到的与多个通信装置210的各个与便携机100之间的距离相关的信息的每一个，进行便携机100的认证。

[0091] 在以下将与距离相关的信息也称为距离相关信息。多个通信装置210的各个基于与便携机100之间的无线通信，获取距离相关信息。

[0092] 控制装置220获取由多个通信装置210得到的多个距离相关信息。而且，控制装置220基于所获取的多个距离相关信息，进行便携机100的认证。详细而言，在多个距离相关信息的任一个满足规定条件的情况下，控制装置220判定为便携机100的认证成功。另一方面，在多个距离相关信息的全部不满足规定条件的情况下，控制装置220判定为便携机100的认证不成立。

[0093] 在以下，作为距离相关信息的一个例子，对第一距离相关信息～第四距离相关信息进行说明。距离相关信息包括第一距离相关信息～第四距离相关信息中的至少任一个。

[0094] 第一距离相关信息

[0095] 距离相关信息也可以是通信装置210与便携机100之间的距离。距离的一个例子是由上述测距处理得到的测距值。

[0096] 多个通信装置210的各个计算与便携机100之间的距离。作为一个例子，多个通信

装置210的各个通过进行上述的测距处理，计算与便携机100之间的距离。

[0097] 控制装置220判定距离相关信息所包含的距离是否满足规定条件，判定便携机100的认证成功与否。规定条件的一个例子是距离相关信息所包含的距离在规定的阈值以下。该情况下，在距离相关信息所包含的距离在规定的阈值以下的情况下，控制装置220判定距离相关信息满足规定条件。另一方面，在距离相关信息所包含的距离超过规定的阈值的情况下，控制装置220判定距离相关信息不满足规定条件。而且，在由多个通信装置210得到的多个距离相关信息的任一个满足规定条件的情况下，控制装置220判定便携机100的认证成功。另一方面，在由多个通信装置210得到的多个距离相关信息的全部不满足规定条件的情况下，控制装置220判定便携机100的认证不成立。

[0098] 第二距离相关信息

[0099] 距离相关信息也可以是用于计算通信装置210与便携机100之间的距离的时间长度。时间长度的一个例子是便携机100与通信装置210之间的单程的测距用信号的收发所需的时间即传播时间。时间长度的另外的一个例子是用于计算传播时间的时间ΔT1以及时间ΔT2。

[0100] 多个通信装置210的各个获取上述时间长度。作为一个例子，多个通信装置210的各个通过进行上述的测距处理中的至少测距通信，获取时间长度。

[0101] 控制装置220基于距离相关信息所包含的时间长度，计算多个通信装置210的各个与便携机100之间的距离。作为一个例子，在距离相关信息所包含的时间长度是传播时间的情况下，控制装置220通过将传播时间乘以信号的速度，计算距离。作为另外的一个例子，在距离相关信息所包含的时间长度是时间ΔT1以及ΔT2的情况下，控制装置220基于ΔT1以及ΔT2首先计算传播时间，并基于所计算出的传播时间计算距离。

[0102] 而且，控制装置220判定所计算出的距离是否满足规定条件，判定便携机100的认证成功与否。规定条件的一个例子是所计算出的距离在规定的阈值以下。该情况下，在所计算出的距离在规定的阈值以下的情况下，控制装置220判定距离相关信息满足规定条件。另一方面，在所计算出的距离超过规定的阈值的情况下，控制装置220判定距离相关信息不满足规定条件。而且，在由多个通信装置210得到的多个距离相关信息的任一个满足规定条件的情况下，控制装置220判定便携机100的认证成功。另一方面，在由多个通信装置210得到的多个距离相关信息的全部不满足规定条件的情况下，控制装置220判定便携机100的认证不成立。

[0103] 第三距离相关信息

[0104] 距离相关信息也可以是用于计算通信装置210与便携机100之间的距离的时刻。时刻的一个例子是时间ΔT1的开始期、即第一测距用信号的发送时刻。时刻的另外的一个例子是时间ΔT1的结束期、即第二测距用信号的接收时刻。时刻的另外的一个例子是时间ΔT2的开始期、即第一测距用信号的接收时刻。时刻的另外的一个例子是时间ΔT2的结束期、即第二测距用信号的发送时刻。

[0105] 多个通信装置210的各个获取上述时刻。作为一个例子，多个通信装置210的各个通过进行上述的测距处理中的至少测距通信，获取时刻。

[0106] 控制装置220基于距离相关信息所包含的时刻，获取用于计算多个通信装置210的各个与便携机100之间的距离的时间长度。时间长度的一个例子是传播时间。时间长度的另

外的一个例子是时间ΔT1以及时间ΔT2。

[0107] 接着，控制装置220基于所获取的时间长度，计算多个通信装置210的各个与便携机100之间的距离。作为一个例子，在所获取的时间长度是传播时间的情况下，控制装置220通过将传播时间乘以信号的速度，计算距离。作为另外的一个例子，在所获取的时间长度是时间ΔT1以及ΔT2的情况下，控制装置220基于ΔT1以及ΔT2首先计算传播时间，并基于所计算出的传播时间而计算距离。

[0108] 而且，控制装置220判定所计算出的距离是否满足规定条件，判定便携机100的认证成功与否。规定条件的一个例子是所计算出的距离在规定的阈值以下。该情况下，在所计算出的距离在规定的阈值以下的情况下，控制装置220判定距离相关信息满足规定条件。另一方面，在所计算出的距离超过规定的阈值的情况下，控制装置220判定距离相关信息不满足规定条件。而且，在由多个通信装置210得到的多个距离相关信息的任一个满足规定条件的情况下，控制装置220判定便携机100的认证成功。另一方面，在由多个通信装置210得到的多个距离相关信息的全部不满足规定条件的情况下，控制装置220判定便携机100的认证不成立。

[0109] 第四距离相关信息

[0110] 距离相关信息也可以是表示通信装置210与便携机100之间的距离是否满足规定条件的信息。

[0111] 多个通信装置210的各个计算出通信装置210与便携机100之间的距离。作为一个例子，多个通信装置210的各个通过进行上述的测距处理，计算出与便携机100之间的距离。

[0112] 接着，多个通信装置210的各个判定通信装置210与便携机100之间的距离是否满足规定条件。规定条件的一个例子是所计算出的距离在规定的阈值以下。该情况下，多个通信装置210的各个判定所计算出的距离是否满足规定条件。而且，在所计算出的距离在规定的阈值以下的情况下，多个通信装置210的各个判定通信装置210与便携机100之间的距离满足规定条件。另一方面，在所计算出的距离超过规定的阈值的情况下，多个通信装置210的各个判定通信装置210与便携机100之间的距离不满足规定条件。

[0113] 而且，控制装置220基于距离相关信息所包含的、表示通信装置210与便携机100之间的距离是否满足规定条件的信息，判定便携机100的认证成功与否。详细而言，在为表示由多个通信装置210得到的多个距离相关信息的任一个满足规定条件的信息的情况下，控制装置220判定便携机100的认证成功。另一方面，在为表示由多个通信装置210得到的多个距离相关信息的全部不满足规定条件的信息的情况下，控制装置220判定便携机100的认证不成立。

[0114] (5)认证结果的用途

[0115] 在第一认证处理中认证成功的情况下，控制装置220执行第二认证处理。另一方面，在第一认证处理中认证失败的情况下，控制装置220判定为便携机100的认证失败。

[0116] 在第二认证处理中认证成功的情况下，控制装置220判定为便携机100的认证成功。另一方面，在第二认证处理中认证失败的情况下，控制装置220判定为便携机100的认证失败。

[0117] 作为一个例子，控制装置220在判定为便携机100的认证成功的情况下，允许或者执行车辆202的车门锁的上锁解锁动作。由此，例如，若在车门上锁时触摸操作车外车门把

手，则车门被解锁，若在车门解锁时按压操作车外车门把手的锁定按钮，则车门被上锁。

[0118] 作为另外的一个例子，控制装置220在判定为便携机100的认证成功的情况下，允许或者执行设置于车辆202的发动机开关引起的发动机动作。由此，例如，若在踩下制动踏板的同时操作发动机开关，则车辆202的发动机启动。

[0119] 此外，控制装置220也可以具有用于车室外的用于无线通信的天线、和用于车室内的无线通信的天线。而且，在借助用于车室外的无线通信，第一认证处理中的认证成功并且第二认证处理也成功的情况下，控制装置220也可以允许或者执行车辆202的车门锁的上锁解锁动作。另一方面，在借助用于车室内的无线通信，第一认证处理中的认证成功并且第二认证处理也成功的情况下，控制装置220也可以允许或者执行设置于车辆202的发动机开关引起的发动机动作。

[0120] (6)处理的流程

[0121] 图4是表示本实施方式所涉及的通信单元200中所执行的第二认证处理的基本的流程的一个例子的流程图。

[0122] 如图4所示，首先，多个通信装置210的各个在与便携机100之间进行测距通信(步骤S302)。测距通信在图3的步骤S202～S206中如上述说明那样。

[0123] 接着，多个通信装置210的各个获取距离相关信息(步骤S304)。详细而言，多个通信装置210的各个基于步骤S302中的测距通信，获取距离相关信息。

[0124] 接下来，控制装置220基于由多个通信装置210得到的多个距离相关信息，进行便携机100的认证(步骤S306)。详细而言，在由多个通信装置210得到的多个距离相关信息的任一个满足规定条件的情况下，控制装置220判定为便携机100的认证成功。另一方面，在由多个通信装置210得到的多个距离相关信息的全部不满足规定条件的情况下，控制装置220判定为便携机100的认证不成立。

[0125] ＜2.2.通信装置与控制装置的连接方式＞

[0126] 通信装置210与控制装置220的连接方式可以考虑多种。以下，参照图5～图7并对通信装置210与控制装置220的连接方式的一个例子进行说明。

[0127] (1)第一连接方式

[0128] 图5是表示本实施方式所涉及的通信装置210与控制装置220的第一连接方式的框图。如图5所示，通信装置210A～210C的各个与控制装置220连接。

[0129] 多个通信装置210的各个发送距离相关信息。控制装置220接收从多个通信装置210的各个发送的距离相关信息。而且，控制装置220基于所接收的距离相关信息，进行便携机100的认证。

[0130] 在这里，如图5所示，通信装置210A～210C的各个与控制装置220之间的通信路径被统一。即，通信装置210A～210C的各个共享与控制装置220之间的通信路径。

[0131] 因此，多个通信装置210的各个在执行了确认到控制装置220的通信路径的空闲的载波侦听的基础上，发送距离相关信息。详细而言，多个通信装置210的各个在通过载波侦听确认了通信路径空闲的情况下，发送距离相关信息。另一方面，多个通信装置210的各个在通过载波侦听确认了通信路径不空闲的情况下，暂时待机。通过上述的结构，能够防止在通信路径上的冲突。

[0132] 此外，作为在执行了载波侦听的基础上发送信息的车载网络的一个例子，列举有

CAN(Controller Area Network:控制器局域网)。

[0133] (2)第二连接方式

[0134] 图6是表示本实施方式所涉及的通信装置210与控制装置220的第二连接方式的框图。如图6所示,通信装置210A～210C的各个与控制装置220连接。

[0135] 多个通信装置210的各个发送距离相关信息。控制装置220接收从多个通信装置210的各个发送的距离相关信息。而且,控制装置220基于所接收的距离相关信息,进行便携机100的认证。

[0136] 在这里,如图6所示,通信装置210A～210C的各个与控制装置220之间的通信路径相互独立。即,通信装置210A～210C的各个在与控制装置220之间分别具有不同的通信路径。

[0137] 多个通信装置210的各个在预先分配给多个通信装置210的每一个的时机,发送距离相关信息。作为一个例子,控制装置220也可以向多个通信装置210的各个分配发送距离相关信息的时机。作为另外的一个例子,多个通信装置210的任一个也可以进行发送距离相关信息的时机的分配。

[0138] 此外,作为在所分配的时机发送信息的车载网络的一个例子,列举有LIN(Local Interconnect Network:局域互联网络)。

[0139] (3)第三连接方式

[0140] 图7是表示本实施方式所涉及的通信装置210与控制装置220的第三连接方式的框图。如图7所示,通信装置210B以及通信装置210C分别与通信装置210A连接。而且,通信装置210A和控制装置220被连接。

[0141] 在第一连接方式中,多个通信装置210包括第一通信装置210以及第二通信装置210。在以下,将第一通信装置210也称为主机210。另外,将第二通信装置210也称为从机210。在图7所示的例子中,通信装置210A是主机210的一个例子。通信装置210B以及通信装置210C是从机210的一个例子。

[0142] 一个以上的从机210的各个与主机210连接。而且,一个以上的从机210的各个发送距离相关信息。此外,从机210与主机210的连接方式也可以如上述的第一连接方式那样,在执行了载波侦听的基础上发送信息。另外,从机210与主机210的连接方式也可以如上述的第二连接方式那样,在所分配的时机发送信息。

[0143] 主机210与一个以上的从机210的各个、以及控制装置220连接。主机210接收从一个以上的从机210的各个发送的距离相关信息。而且,主机210发送由主机210得到的距离相关信息、以及从一个以上的从机210的各个接收到的距离相关信息的至少任一个所对应的信息、即对应信息。

[0144] 控制装置220接收从主机210发送的对应信息。而且,控制装置220基于所接收的对应信息,进行便携机100的认证。

[0145] 根据本连接方式,控制装置220能够将对应信息设为处理对象,而不是将由主机210得到的距离相关信息、以及由一个以上的从机210的各个得到的一个以上的距离相关信息的全部设为处理对象。因此,期待能够简化控制装置220中的处理。

[0146] ＜2.3.通信单元内通信＞

[0147] 在以下,假定第三连接方式,对关于通信单元200内的通信的技术的特征进行说

明。

[0148] 在这里，距离相关信息是第四距离相关信息。即，距离相关信息是表示通信装置210与便携机100之间的距离是否满足规定条件的信息。而且，主机210在多个通信装置210(主机210以及从机210)的任一个中，发送表示与便携机100之间的距离是否满足规定条件的信息作为对应信息。具体而言，在主机210以及从机210中的测距值的任一个满足规定条件的情况下，主机210发送表示满足规定条件的信息作为对应信息。另一方面，在主机210以及从机210中的测距值的全部不满足规定条件的情况下，主机210发送表示不满足规定条件的信息作为对应信息。

[0149] 控制装置220若从主机210接收对应信息，则基于所接收的对应信息进行便携机100的认证。例如，在对应信息包括表示满足规定条件的信息的情况下，控制装置220判定为便携机100的认证成功。另一方面，在对应信息包括表示不满足规定条件的信息的情况下，控制装置220判定为便携机100的认证不成立。

[0150] 此外，主机210也可以对对应信息进行加密而发送。例如，主机210也可以利用通用密钥密码方式将对应信息进行加密。通用密钥密码方式是在加密和解密中使用相同的密钥的密码方式。也就是说，主机210和控制装置220使用相同的密钥。通过上述的结构，能够防止有恶意的第三者的冒充，使安全性提高。

[0151] 同样地，从机210也可以对距离相关信息进行加密而发送。例如，从机210也可以通过通用密钥密码方式对距离相关信息进行加密。通用密钥密码方式是在加密和解密中使用相同的密钥的密码方式。也就是说，从机210和主机210使用相同的密钥。通过上述的结构，能够使安全性提高。

[0152] 此外，在通用密钥密码方式中，密钥也可以是随机数。在密钥为随机数的情况下，随机数在加密侧和解密侧基于相同的种子被生成。种子例如是每次生成时值不同的随机数。由此，能够在加密侧和解密侧使用相同的随机数作为密钥。密钥也可以被随时更新。例如，密钥也可以在每次执行测距处理时被更新。

[0153] 主机210也可以在自从机210接收距离相关信息之前，计算主机210与便携机100之间的距离。该情况下，在所计算出的距离满足规定条件的情况下，主机210发送表示与便携机100之间的距离是否满足规定条件的信息作为对应信息。另一方面，在所计算出的距离不满足规定条件的情况下，主机210在自从机210接收了距离相关信息的基础上，发送对应信息。即，在主机210中的测距值满足规定条件的情况下，主机210不等待自从机210接收距离相关信息，就发送对应信息。因此，能够使第二认证处理的响应性提高。

[0154] (1)从机－主机间的通信的特征

[0155] 从机210也可以预先生成距离相关信息的候选，将与在测距处理中计算出的距离(即，测距值)对应的候选作为距离相关信息发送。这里的距离相关信息是表示从机210与便携机100之间的距离是否满足规定条件的信息。距离相关信息的候选也是表示从机210与便携机100之间的距离是否满足规定条件的信息。但是，距离相关信息的候选在得到测距值之前被生成，因此标注“候选”。预先生成的距离相关信息的候选包括以下说明的第一候选以及第二候选。

[0156] 详细而言，从机210通过将表示从机210与便携机100的距离满足规定条件的信息进行加密，生成距离相关信息的第一候选。也就是说，距离相关信息的第一候选是对表示从

机210与便携机100的距离满足规定条件的信息进行加密后的信息。而且，从机210在进行了测距处理后，在测距值满足规定条件的情况下，将距离相关信息的第一候选作为距离相关信息发送。另一方面，从机210通过对表示从机210与便携机100的距离不满足规定条件的信息进行加密，生成距离相关信息的第二候选。也就是说，距离相关信息的第二候选是对表示从机210与便携机100的距离不满足规定条件的信息进行加密后的信息。而且，从机210在进行了测距处理后，在测距值不满足规定条件的情况下，将距离相关信息的第二候选作为距离相关信息发送。

[0157] 根据上述的结构，在进行测距处理之前已经生成距离相关信息的候选，因此能够缩短从进行测距处理之后直到发送距离相关信息为止的时间。因此，能够使第二认证处理的响应性提高。

[0158] 另一方面，主机210也可以预先生成自从机210接收的距离相关信息的候选。而且，主机210也可以发送所生成的距离相关信息的候选与自从机210接收的距离相关信息的比较结果所对应的对应信息。例如，主机210预先生成自从机210接收的距离相关信息的第一候选以及第二候选。而且，主机210基于实际自从机210接收的距离相关信息与预先生成的第一候选以及第二候选的任一个是否一致，来识别从机210与便携机100的距离是否满足规定条件。根据上述的结构，主机210能够不对加密后的距离相关信息进行解密，就识别从机210中的测距值是否满足规定条件。因而，能够缩短从主机210接收距离相关信息之后直到主机210发送对应信息为止的时间。因此，能够使第二认证处理的响应性提高。

[0159] 对于上述说明的点，参照图8并进行详细说明。图8是表示本实施方式所涉及的主机210与从机210之间的信息的流程的一个例子的图。从机210预先生成距离相关信息“A”以及“B”作为距离相关信息的候选。距离相关信息“A”是对表示测距值满足规定条件的信息进行加密后的信息。即，距离相关信息“A”是距离相关信息的第一候选。另一方面，距离相关信息“B”是对表示测距值不满足规定条件的信息进行加密后的信息。即，距离相关信息“B”是距离相关信息的第二候选。同样地，主机210预先生成距离相关信息“A”以及“B”作为距离相关信息的候选。

[0160] 从机210在执行测距处理后，发送与测距值对应的距离相关信息的候选。详细而言，如图8的上段所示，从机210在测距值满足规定条件的情况下发送距离相关信息“A”。另一方面，如图8的下段所示，从机210在测距值不满足规定条件的情况下发送距离相关信息“B”。

[0161] 主机210对预先生成的距离相关信息“A”及“B”和自从机210接收的距离相关信息进行比较。而且，如图8的上段所示，在预先生成的距离相关信息“A”与自从机210接收的距离相关信息一致的情况下，主机210识别为该从机210中的测距值满足规定条件。另一方面，如图8的下段所示，在预先生成的距离相关信息“B”与自从机210接收的距离相关信息一致的情况下，主机210识别为该从机210中的测距值不满足规定条件。

[0162] (2)主机－控制装置间的通信的特征

[0163] 主机210也可以预先生成对应信息的候选，将所计算出的距离以及自从机210接收到的距离相关信息所对应的候选作为对应信息发送。这里的对应信息是表示在多个通信装置210(主机210以及从机210)的任一个中，与便携机100之间的距离是否满足规定条件的信息。对应信息的候选也是表示在多个通信装置210(主机210以及从机210)的任一个中，与便

携机100之间的距离是否满足规定条件的信息。但是，对应信息的候选在主机210中得到测距值之前、或者在主机210自从机210接收距离相关信息之前被生成，因此标注“候选”。预先生成的对应信息的候选包括以下说明的第一候选以及第二候选。

[0164] 详细而言，主机210通过对表示主机210以及从机210中的测距值的任一个满足规定条件的信息进行加密，生成对应信息的第一候选。而且，主机210在进行测距处理，并自从机210接收距离相关信息之后，在主机210以及从机210中的测距值的任一个满足规定条件的情况下，发送对应信息的第一候选作为对应信息。另一方面，主机210通过对表示主机210以及从机210中的测距值的全部不满足规定条件的信息进行加密，生成对应信息的第二候选。而且，主机210在进行测距处理，并自从机210接收距离相关信息之后，在主机210以及从机210中的测距值的全部不满足规定条件的情况下，发送对应信息的第二候选作为对应信息。

[0165] 根据上述的结构，在接收测距处理以及距离相关信息之前已经生成对应信息的候选，因此能够缩短从接收测距处理以及距离相关信息之后直到发送对应信息为止的时间。因此，能够使第二认证处理的响应性提高。

[0166] 另一方面，控制装置220也可以预先生成从主机210接收的对应信息的候选。而且，控制装置220也可以根据所生成的对应信息的候选与从主机210接收的对应信息的比较结果，进行便携机100的认证。例如，控制装置220预先生成对应信息的第一候选以及第二候选。而且，控制装置220基于从主机210接收的对应信息与第一候选以及第二候选的任一个是否一致，来识别主机210以及从机210中的测距值是否满足规定条件。根据上述的结构，控制装置220能够不对加密后的对应信息进行解密，就识别出主机210以及从机210中的测距值是否满足规定条件。因而，能够缩短从控制装置220接收对应信息之后直到控制装置220进行便携机100的认证为止的时间。因此，能够使第二认证处理的响应性提高。

[0167] 对于上述说明的点，参照图9并进行详细说明。图9是表示本实施方式所涉及的控制装置220与主机210之间的信息流的一个例子的图。主机210预先生成对应信息“C”以及“D”作为对应信息的候选。对应信息“C”是对表示主机210以及从机210中的测距值的任一个满足规定条件的信息进行加密后的信息。即，对应信息“C”是对应信息的第一候选。另一方面，对应信息“D”是对表示主机210以及从机210中的测距值的全部不满足规定条件的信息进行加密后的信息。即，对应信息“D”是对应信息的第二候选。同样地，控制装置220预先生成对应信息“C”以及“D”作为对应信息的候选。

[0168] 主机210在执行测距处理，并自从机210接收了距离相关信息后，发送主机210以及从机210中的测距值所对应的对应信息的候选。详细而言，如图9的上段所示，在主机210以及从机210中的测距值的任一个满足规定条件的情况下，主机210发送对应信息“C”。另一方面，如图9的下段所示，在主机210以及从机210中的测距值的全部不满足规定条件的情况下，主机210发送对应信息“D”。

[0169] 控制装置220对预先生成的对应信息“C”及“D”和从主机210接收的对应信息进行比较。而且，如图9的上段所示，在预先生成的对应信息“C”与从主机210接收的对应信息一致的情况下，控制装置220识别为主机210以及从机210中的测距值的任一个满足规定条件。另一方面，如图9的下段所示，在预先生成的对应信息“D”与从主机210接收的对应信息一致的情况下，控制装置220识别为主机210以及从机210中的测距值的全部不满足规定条件。

[0170] 但是，主机210在接收到的距离相关信息不正当的情况下，将表示接收到的距离相关信息不正当的信息作为对应信息发送。接收到的距离相关信息不正当的一个例子是在主机210中预先生成的距离相关信息的候选与自从机210接收的距离相关信息不一致。这样的不正当的距离相关信息在从机210与便携机100之间的通信中产生错误的情况下、或者在主机210与从机210之间的通信中产生错误的情况下能够被接收。在这一点上，通过上述的结构，控制装置220能够检测通信中产生的异常。

[0171] 另外，这样的不正当的距离相关信息在有恶意的第三者尝试冒充的情况下能够被接收。因此，控制装置220也可以在对应信息表示距离相关信息不正当的情况下，判定便携机100的认证不成立。通过上述的结构，能够使安全性提高。

[0172] 对于上述说明的点，参照图10并进行详细说明。图10是表示本实施方式所涉及的通信单元200中的信息流的一个例子的图。参照图8并如上述说明那样，主机210预先生成距离相关信息“A”以及“B”作为自从机210接收的距离相关信息的候选。距离相关信息“A”是对表示测距值满足规定条件的信息进行加密后的信息。另一方面，距离相关信息“B”是对表示测距值不满足规定条件的信息进行加密后的信息。主机210自从机210接收不正当的距离相关信息“E”。该情况下，主机210判定为预先生成的距离相关信息“A”以及“B”的任一个与自从机210接收的距离相关信息“E”不一致。而且，主机210将表示自从机210接收的距离相关信息不正当的信息“F”作为对应信息发送。

[0173] 此外，除了表示主机210以及正常的从机210中的测距值是否满足规定条件的信息之外，主机210也可以将表示所接收的距离相关信息不正当的信息作为对应信息发送。正常的从机210是发送正常的距离相关信息的从机210。例如，在图8～图10所示的例子中，主机210也可以发送“C”+“F”或者“D”+“F”作为对应信息。通过上述的结构，控制装置220能够基于产生异常的从机210以外的测距值，进行便携机100的认证。

[0174] (3)总结

[0175] 将以上说明的主机210以及从机210中的测距值与通知给控制装置220的对应信息的关系表示在下述表1中。

[0176] 【表1】

[0177] 表1.主机以及从机中的测距值与对应信息的关系

[0178]

对应信息	主机中的测距值	从机中的测距值
OK (对应信息：C)	OK	OK
	OK	NG
	NG	OK
NG (对应信息：D)	NG	NG
OK＋不正当 (对应信息：C＋F)	OK	不正当
NG＋不正当 (对应信息：D＋F)	NG	不正当

[0179] 在上述表1中，“从机中的测距值”一栏的“OK”表示从机210中的测距值满足规定条件。“从机中的测距值”一栏的“NG”表示从机210中的测距值不满足规定条件。“从机中的测距值”一栏的“不正当”表示主机210自从机210接收的距离相关信息不正当。“主机中的测距值”一栏的“OK”表示主机210中的测距值满足规定条件。“主机中的测距值”一栏的“NG”表示

主机210中的测距值不满足规定条件。

[0180] “对应信息”一栏的“OK”表示对应信息是表示主机210以及从机210中的测距值的任一个满足规定条件的信息。如上述表1所示，如果“主机中的测距值”一栏或者“从机中的测距值”一栏的任一个是“OK”，则对应信息一栏成为“OK”。也就是说，“对应信息”一栏的“OK”相当于图9的上段所示的对应信息“C”。

[0181] “对应信息”一栏的“NG”表示对应信息是表示主机210以及从机210中的测距值的全部不满足规定条件的信息。如上述表1所示，如果“主机中的测距值”一栏以及“从机中的测距值”一栏的双方为“NG”，则对应信息一栏成为“NG”。“对应信息”一栏的“NG”相当于图9的下段所示的对应信息“D”。

[0182] “对应信息”一栏的“不正当”表示对应信息是表示来自从机210的距离相关信息不正当的信息。对应信息除了表示来自从机210的距离相关信息不正当的信息之外，还可以包含表示主机210以及正常的从机210中的测距值是否满足规定条件的信息。“对应信息”一栏的“OK+不正当”相当于图9的上段所示的对应信息“C”、以及图10所示的对应信息“F”。“对应信息”一栏的“NG+不正当”相当于图9的下段所示的对应信息“D”、以及图10所示的对应信息“F”。

[0183] (4)处理的流程

[0184] 以下，参照图11并对第二认证处理中的与通信单元200内的通信相关的处理的流程进行说明。图11是表示本实施方式所涉及的通信单元200中所执行的第二认证处理的详细的流程的一个例子的时序图。如图11所示，在本时序图中，涉及控制装置220、主机210A、以及从机210B。在本时序图中，从机210是一个。

[0185] 首先，从机210B生成距离相关信息的候选(步骤S402)。例如，从机210B通过对表示从机210B中的测距值满足规定条件的信息进行加密，生成距离相关信息的第一候选。另外，从机210B通过对表示从机210B中的测距值满足规定条件的信息进行加密，生成距离相关信息的第二候选。

[0186] 同样地，主机210A生成距离相关信息的候选(步骤S404)。

[0187] 另外，主机210A生成对应信息的候选(步骤S406)。例如，主机210A通过对表示主机210A以及从机210B中的测距值的任一个满足规定条件的信息进行加密，生成对应信息的第一候选。另外，主机210A通过对表示主机210A以及从机210B中的测距值的全部不满足规定条件的信息进行加密，生成对应信息的第二候选。

[0188] 同样地，控制装置220生成对应信息的候选(步骤S408)。

[0189] 接着，主机210A以及从机210B在与便携机100之间进行测距处理(步骤S410)。由此，主机210A以及从机210B的各个获取与便携机100之间的距离的测定结果作为测距值。

[0190] 接下来，主机210A判定由主机210A得到的测距值是否满足规定条件(步骤S412)。在判定为由主机210A得到的测距值满足规定条件的情况下(步骤S412:是)，主机210A发送表示测距值满足规定条件的对应信息、即对应信息的第一候选(步骤S414)。

[0191] 另一方面，在判定为由主机210A得到的测距值不满足规定条件的情况下(步骤S412:否)，主机210A等待来自从机210B的距离相关信息。接着，从机210B判定由从机210B得到的测距值是否满足规定条件(步骤S416)。

[0192] 在判定为由从机210B得到的测距值满足规定条件的情况下(步骤S416:是)，从机

210B发送表示测距值满足规定条件的距离相关信息、即距离相关信息的第一候选(步骤S418)。接着,主机210发送表示测距值满足规定条件的对应信息、即对应信息的第一候选作为自从机210B接收的距离相关信息所对应的对应信息(步骤S420)。详细而言,所接收到的距离相关信息与表示测距值满足规定条件的距离相关信息的第一候选一致,因此主机210A发送表示测距值满足规定条件的对应信息的第一候选。

[0193] 另一方面,在判定为由从机210B得到的测距值不满足规定条件的情况下(步骤S416:否),从机210B发送表示测距值不满足规定条件的距离相关信息、即距离相关信息的第二候选(步骤S422)。接着,主机210发送表示测距值不满足规定条件的对应信息、即对应信息的第二候选作为自从机210B接收的距离相关信息所对应的对应信息(步骤S424)。详细而言,所接收到的距离相关信息与表示测距值不满足规定条件的距离相关信息的第二候选一致,因此主机210A发送表示测距值不满足规定条件的对应信息的第二候选。

[0194] 然后,控制装置220基于所接收的对应信息,进行便携机100的认证(步骤S426)。详细而言,控制装置220在所接收的对应信息与表示测距值满足规定条件的对应信息的第一候选一致的情况下,判定便携机100的认证成功。另一方面,控制装置220在所接收的对应信息与表示测距值不满足规定条件的对应信息的第二候选一致的情况下,判定便携机100的认证不成立。

[0195] <<3.补充>>

[0196] 以上,参照附图并对本发明的优选的实施方式进行了详细说明,但本发明并不限定于上述的例子。可以理解如果是具有本发明所属的技术领域中的通常的知识的人员,则在权利要求书所记载的技术思想的范畴内,能够想到各种变更例或者修正例是不言而喻的,对于这些,当然也属于本发明的技术范围。

[0197] 例如,在上述实施方式中,对第三连接方式中的与通信单元200内的通信相关的技术的特征进行了说明,但在其他的连接方式中也能够应用同样的技术。

[0198] 作为一个例子,多个通信装置210的各个也可以对距离相关信息进行加密而发送。通过上述的结构,能够使安全性提高。

[0199] 作为另外的一个例子,多个通信装置210的各个也可以预先生成表示与便携机100之间的距离是否满足规定条件的信息的候选,将在测距处理中计算出的距离(即,测距值)所对应的候选作为距离相关信息发送。详细而言,多个通信装置210的各个生成对表示测距值满足规定条件的信息进行加密后的信息、以及对表示测距值不满足规定条件的信息进行加密后的信息作为距离相关信息的候选。而且,多个210的各个发送由测距处理得到的测距值所对应的候选。根据上述的结构,在进行测距处理之前已经生成距离相关信息,因此能够缩短从进行测距处理之后直到发送距离相关信息为止的时间。因此,能够使第二认证处理的响应性提高。

[0200] 该情况下,控制装置220也可以预先生成距离相关信息的候选。而且,控制装置220也可以根据所生成的距离相关信息的候选与从多个通信装置210的各个接收的距离相关信息的比较结果,进行便携机100的认证。例如,控制装置220预先生成距离相关信息的第一候选以及第二候选。而且,控制装置220基于从多个通信装置210的各个接收的距离相关信息与第一候选以及第二候选的任一个是否一致,来识别多个通信装置210的各个中的测距值是否满足规定条件。根据上述的结构,控制装置220能够不对加密后的距离相关信息进行解

密，就识别出通信装置210中的测距值是否满足规定条件。因而，能够缩短从控制装置220接收距离相关信息之后直到控制装置220进行便携机100的认证为止的时间。因此，能够使第二认证处理的响应性提高。

[0201] 除此之外，例如，在上述实施方式中，对被认证者是便携机100、认证者是通信单元200的例子进行了说明，但本发明并不限定于上述的例子。便携机100以及通信单元200的作用也可以相反，也可以动态交换作用。另外，也可以在通信单元200彼此进行测距以及认证。

[0202] 除此之外，例如，在上述实施方式中，对将本发明应用于智能钥匙系统中的例子进行了说明，但本发明并不限定于上述的例子。本发明能够应用于通过收发信号而进行测距以及认证的任意的系统中。例如，本发明能够应用于便携机、车辆、智能手机、无人驾驶飞机、家、以及家电产品等中包含任意两个装置的成对装置。该情况下，成对装置中的一方作为认证者进行动作，另一方作为被认证者进行动作。此外，成对装置可以包含两个相同的种类的装置，也可以包含两个不同的种类的装置。

[0203] 除此之外，例如，在上述实施方式中，列举了使用UHF/LF作为第一无线通信标准，列举了使用UWB作为第二无线通信标准，但本发明并不限定于上述的例子。例如，作为第一无线通信标准，也可以使用Wi-Fi(注册商标)、以及Bluetooth(注册商标)等。另外，例如，作为第二无线通信标准，也可以使用利用了红外线的装置。

[0204] 除此之外，例如，在上述中，说明了在车辆202中搭载有通信单元200，但本发明并不限定于上述的例子。例如，也可以在车辆202的停车场设置通信单元200等，通信单元200的一部分或者全部与车辆202分体构成。该情况下，通信单元200能够基于与便携机100的通信结果，向车辆202无线发送控制信号，远程控制车辆202。

[0205] 此外，基于本说明书中说明的各装置的一系列的处理也可以使用软件、硬件、以及软件与硬件的组合的任一种来实现。构成软件的程序例如被预先储存于记录介质(非暂时的介质:non-transitory media)，该记录介质设置于各装置的内部或者外部。而且，各程序例如在利用计算机执行时被读入RAM，由CPU等处理器执行。上述记录介质例如是磁盘、光盘、光磁盘、闪存等。另外，上述的计算机程序也可以不使用记录介质，例如经由网络进行分发。

[0206] 另外，本说明书中使用流程图以及时序图进行了说明的处理也可以未必根据所图示的顺序执行。几个处理步骤也可以并行执行。另外，可以采用追加的处理步骤，也可以省略一部分处理步骤。

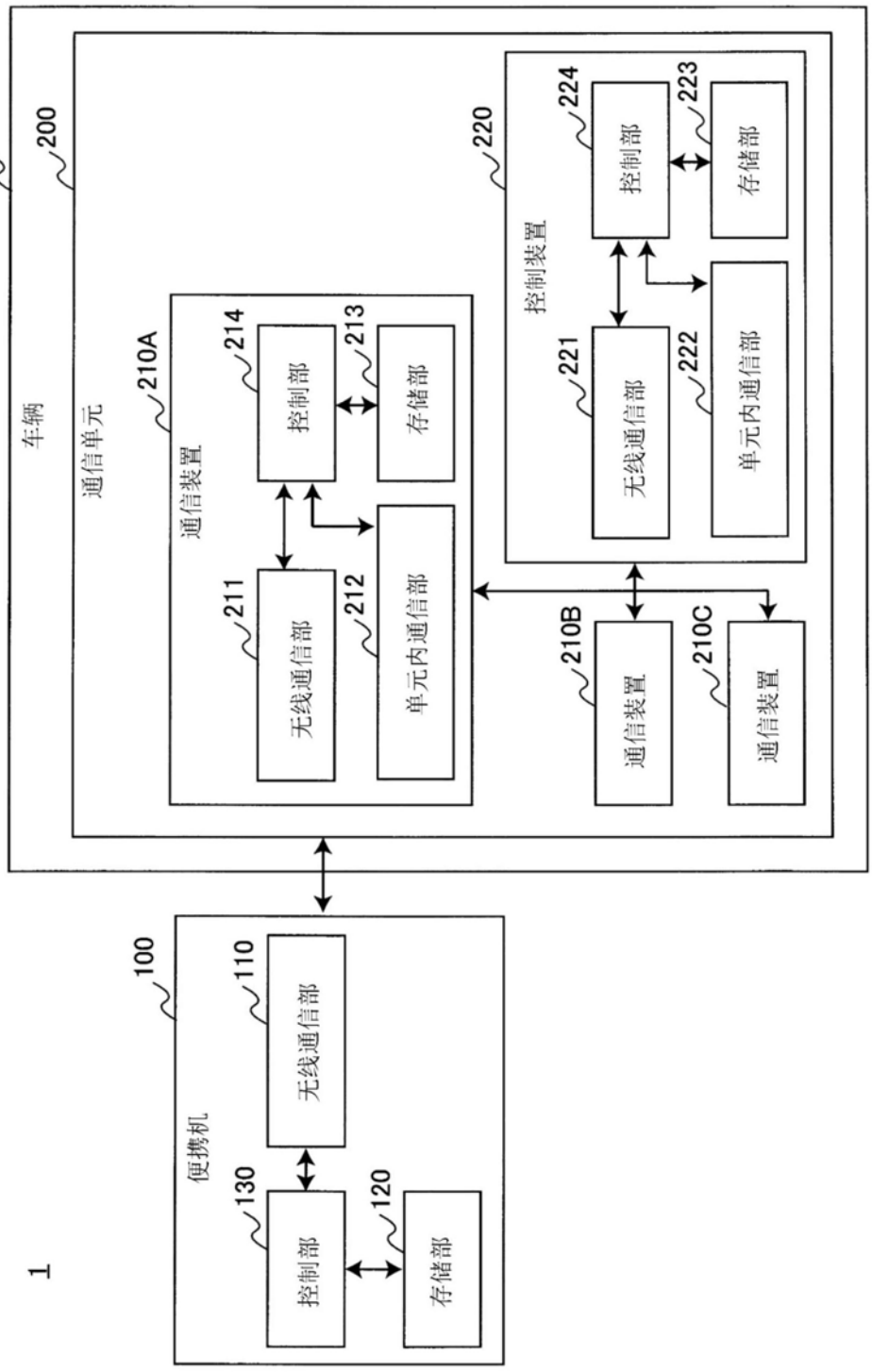

1
便携机
100
控制部
130
存储部
120
无线通信部
110
车辆
202
通信单元
200
通信装置
210A
无线通信部
211
控制部
214
单元内通信部
212
存储部
213
控制装置
220
通信装置
210B
无线通信部
221
控制部
224
单元内通信部
222
存储部
223
通信装置
210C

图1

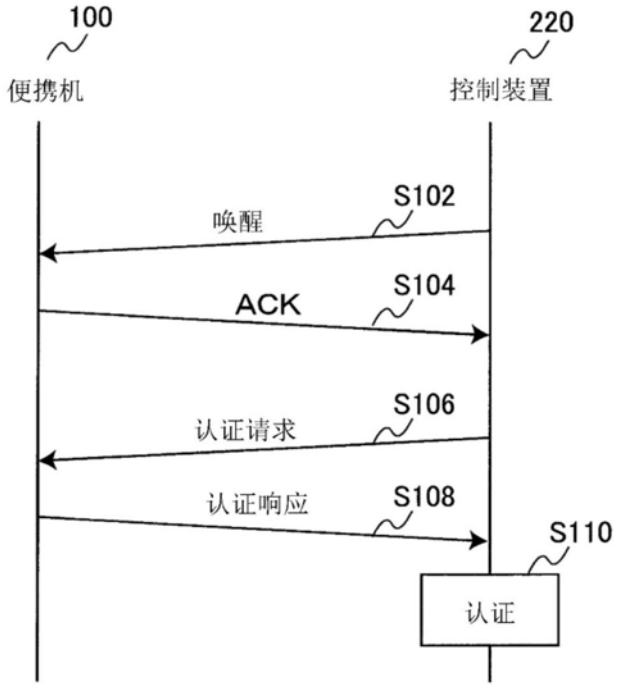

100
便携机
220
控制装置
S102
唤醒
S104
ACK
S106
认证请求
S108
认证响应
S110
认证

图2

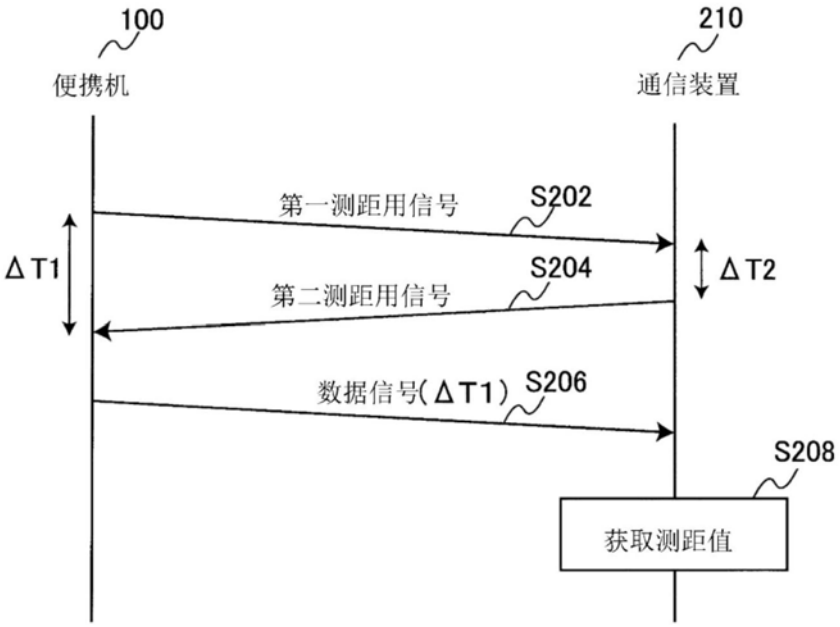

100
便携机
210
通信装置
第一测距用信号
S202
ΔT1
ΔT2
S204
第二测距用信号
数据信号(ΔT1)
S206
S208
获取测距值

图3

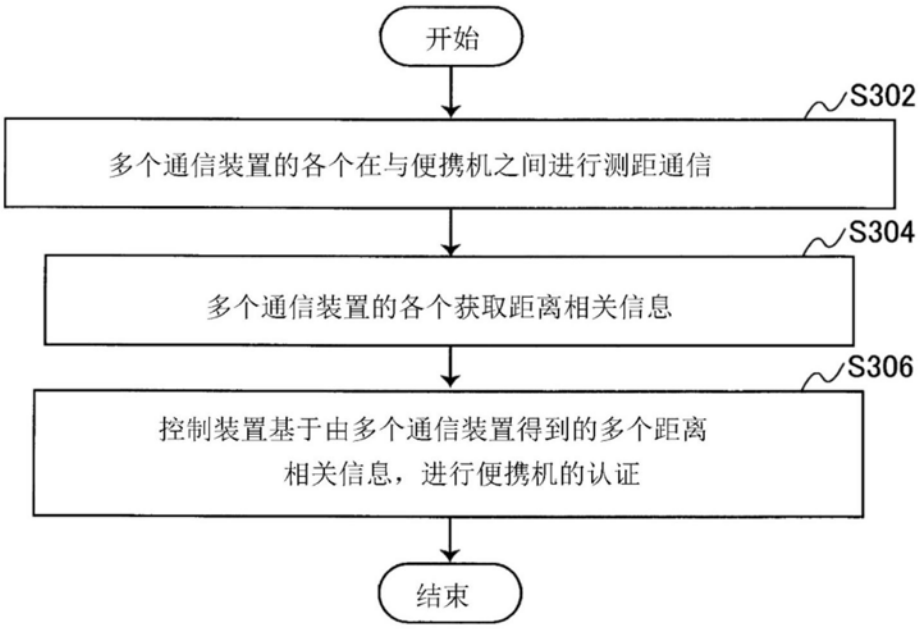

开始
S302
多个通信装置的各个在与便携机之间进行测距通信
S304
多个通信装置的各个获取距离相关信息
S306
控制装置基于由多个通信装置得到的多个距离
相关信息，进行便携机的认证
结束

图4

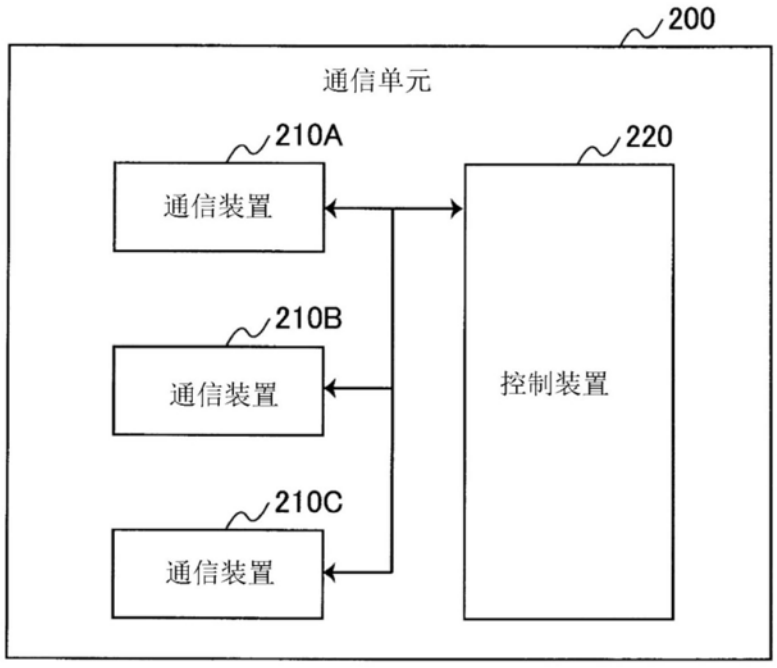

200
通信单元
210A
通信装置
210B
通信装置
210C
通信装置
220
控制装置

图5

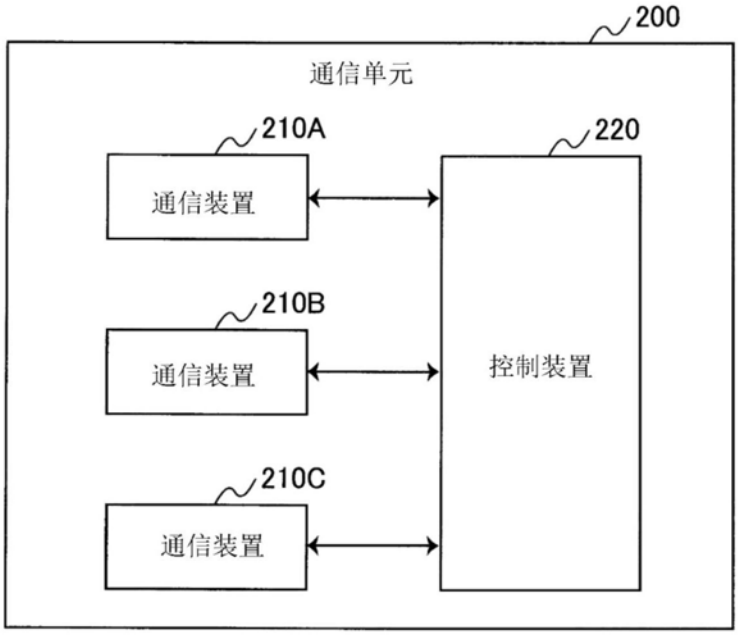

200
通信单元
210A
通信装置
220
210B
通信装置
控制装置
210C
通信装置

图6

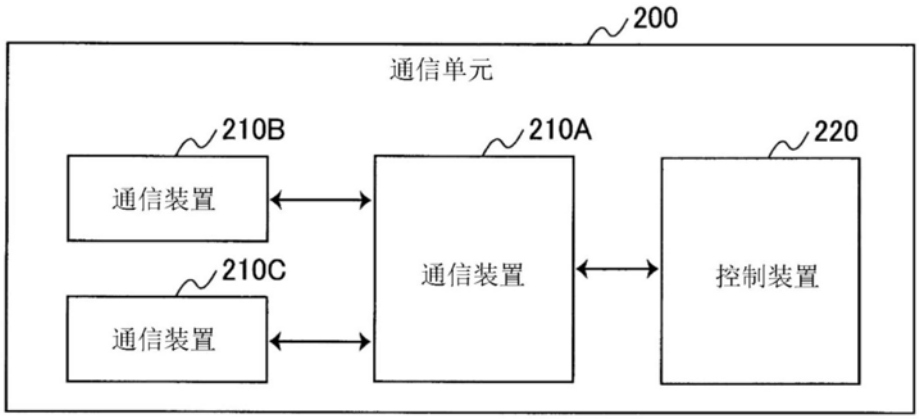

200
通信单元
210B
通信装置
210A
220
210C
通信装置
通信装置
控制装置

图7

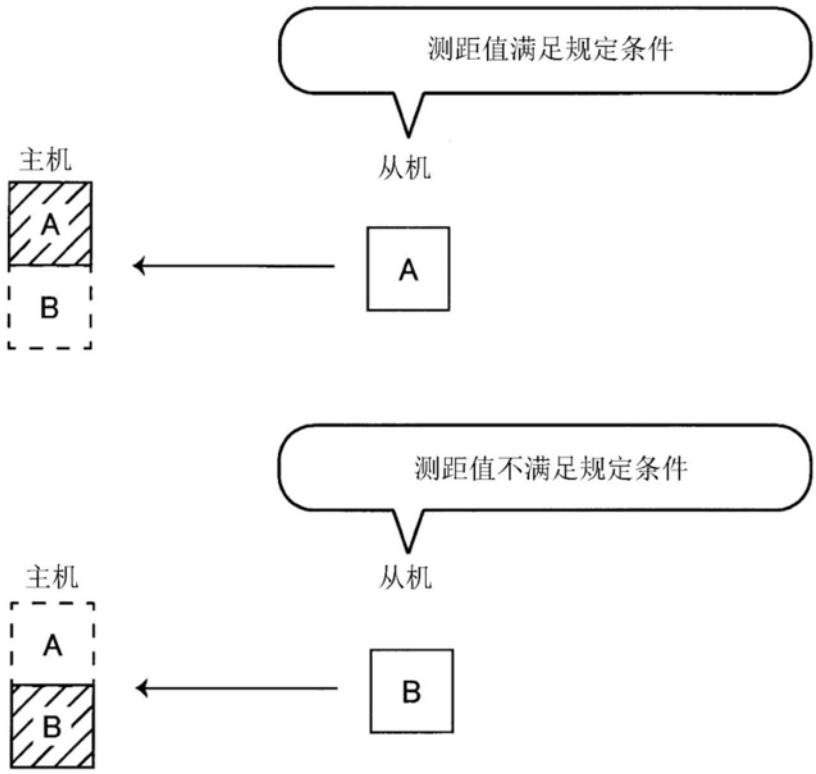


图8

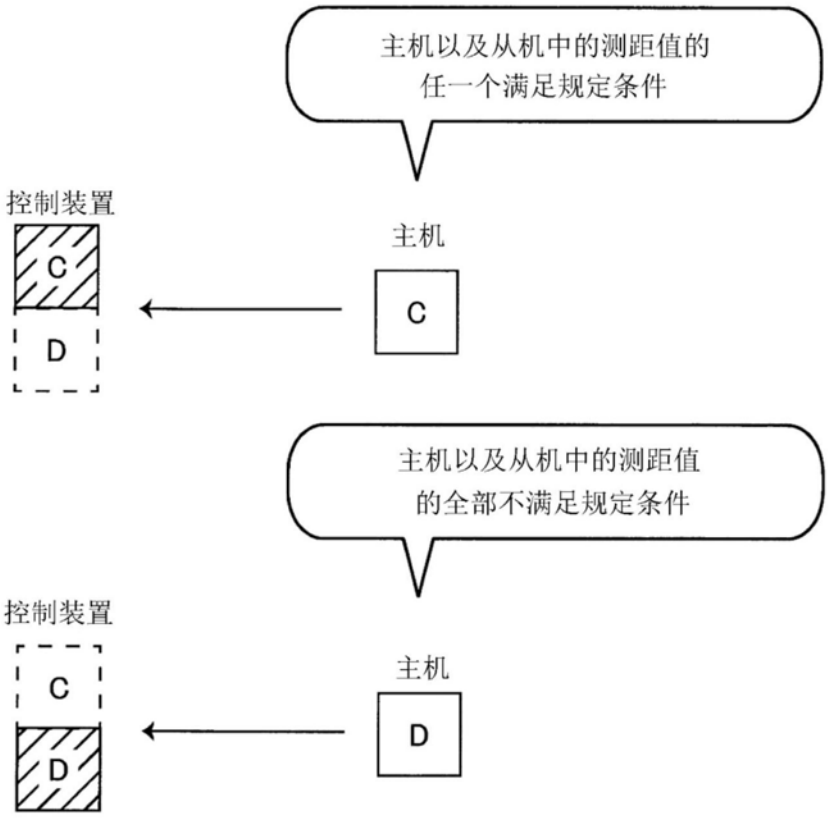

主机以及从机中的测距值的
任一个满足规定条件
控制装置
C
D
主机
C
主机以及从机中的测距值
的全部不满足规定条件
控制装置
C
D
主机
D

图9

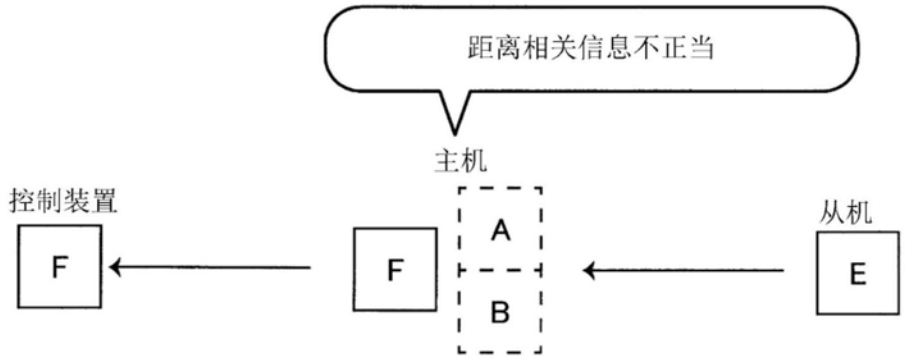

距离相关信息不正当
主机
控制装置
F
F
A
B
从机
E

图10

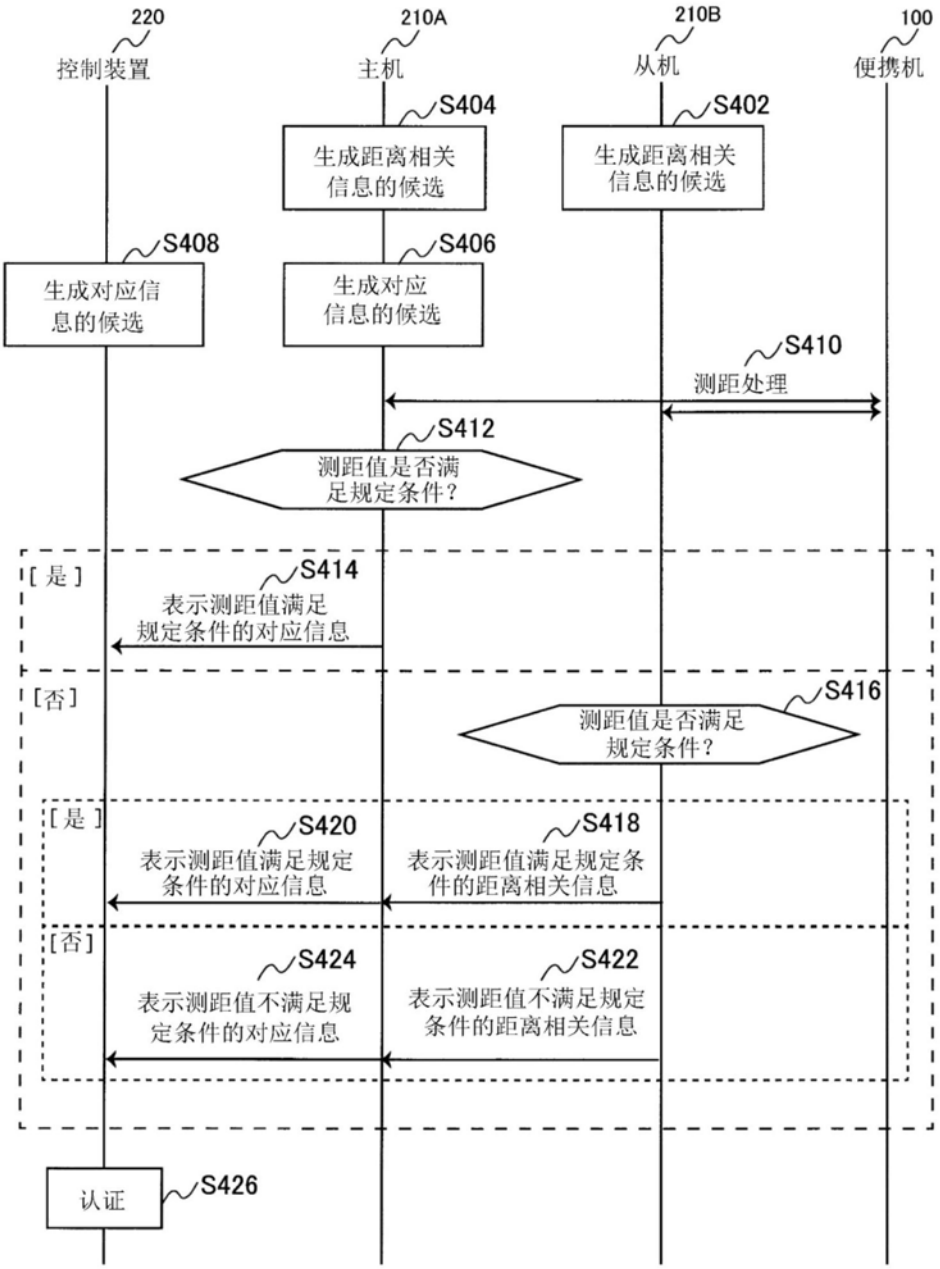

220
控制装置
210A
主机
210B
从机
100
便携机
S404
生成距离相关信息的候选
S402
生成距离相关信息的候选
S408
生成对应信息的候选
S406
生成对应信息的候选
S410
测距处理
S412
测距值是否满足规定条件？
[是]
S414
表示测距值满足规定条件的对应信息
[否]
S416
测距值是否满足规定条件？
[是]
S420
表示测距值满足规定条件的对应信息
S418
表示测距值满足规定条件的距离相关信息
[否]
S424
表示测距值不满足规定条件的对应信息
S422
表示测距值不满足规定条件的距离相关信息
认证
S426

图11